A Delay in the Safeguards Rule, But Dealers Should Not Wait
By Hao Nguyen, Esq.Chief Legal Officer, ComplyAuto

In this article, we discuss the Federal Trade Commission's ("FTC") delay of the effective date of the revised Safeguards Rule ("Rule") and its practical impact to your dealerships. We will then explain why you should not wait to implement data protection and cybersecurity safeguards at your dealership because the FTC will still come after you under another section of the FTC Act that gives them broad authority.

Safeguards Rule – *Some* Requirements Delayed Until June 9, 2023

The FTC gave dealers across the country an early Christmas present when it announced on November 15, 2022 that it is extending the deadline for the Rule by six months. However, it is important to note that this extension *only affects some of the requirements* and will make them effective on June 9, 2023. Specifically, the provisions that have been extended to June include the following:

- Designating a qualified individual to oversee the information security program;
- Completing written risk assessments;
- Monitoring the access and use of sensitive customer information;
- Completing a penetration test & vulnerability scan;
- Encrypting systems containing customer information;
- Training employees on security awareness;
- Conducting Vendor & Service Provider risk assessments;
- Implementing multi-factor authentication (MFA) on all systems containing customer information; and
- Creating and updating a device and systems inventory.

Notably, the provisions that have ***not*** been delayed (and never were) are:

- Creating a written Information Security Program (ISP) for your organization;
- Obtaining signed contracts from your vendors ("Service Providers") who collect customer information promising to implement reasonable safeguards;
- Periodically assessing your Service Providers to ensure that they have reasonable safeguards in place; and
- Implementing a system capable of detecting attacks and intrusions on your network.

Dealers Should Not Wait to Implement Safeguards Rule Solutions

On paper, the delay sounded good. However, once you dig into the details, the delay is not *as* sweet as it sounds. Because some aspects of the Rule still became effective in January of last year, dealers should not take this delay for granted. This is the time to press on in reinforcing their data protection and cybersecurity practices. Why?

Firstly, completing all requirements of the Rule can be time consuming because so many players are involved. You will need to coordinate with the vendor to oversee compliance (like ComplyAuto), the dealership staff, any Service Providers they work with (to complete their requirements), and potentially your IT company or Managed Service Provider. Unless you are working with an efficient and responsive team, natural bottlenecks may arise as one party waits on the other.

Secondly, you should not "miss the forest for the trees," meaning that the FTC should not be the main reason why your dealership is establishing these data protection and cybersecurity protocols. Yes, we want to fulfill these requirements to keep the federal government at bay, but I would argue that **the main focus should be to prevent data breaches, ransomware attacks, or other cybersecurity incidents!** Think about the different forms of damage to your organization that could arise as a result of a data breach or ransomware attack:

- Reputational damage. Dealerships are pillars in their community and word of a data breach will spread quickly. Additionally, vendors may be wary about working with you in the future.
- Data breach mitigation. Depending on the level of your cybersecurity coverage from your insurance company (or lack thereof), you could be paying out of pocket for forensic professionals to "stem the bleeding", so to speak, and try and recover what you can.
- Dealership downtime. You can bet that your dealership will suffer significant delays as you try to survey the extent of the breach and work through the mitigation efforts.
- Data recovery. If it was a ransomware attack that resulted in the loss of employee, customer, and dealership information, the road back to where you started will be a long one. Think of all the information that existed prior to the attack that you will now need to rebuild from scratch.
- Consumer protection efforts. Depending on the extent of the breach, you may be legally responsible for the cost of providing identity theft protection measures to all of the consumers who suffered a release of their information.

- State and federal penalties. Suffering a breach does not earn you any pity from the government. State and federal enforcement officials will come in shortly thereafter to "pour salt in the wound" in the form of heavy fines and penalties.
- Class actions lawsuits. Always a significant concern for dealers is a class action lawsuit by harmed individuals who had their information either stolen or released.

FTC Using its Broad Authority under Section 5 for Cybersecurity Concerns

Section 5 of the FTC Act prohibits "unfair or deceptive business practices in or affecting commerce." Given that this clause has been around since 1914, it is safe to say that the authors did not consider cybersecurity during the time that it was drafted. Nevertheless, as a Nobel Prize laureate once said, "the times they are a changin'' and the FTC has wielded this section as a sword to strike down businesses who have displayed poor cybersecurity practices. This has become such an issue that Brad Miller, Chief Regulatory Counsel at NADA, spoke about this during one of the educational seminars at the Dallas convention.

Defining false data security or privacy representations under both "unfair" and "deceptive" terms of art since 2002, the FTC has negotiated consent agreements since then with most businesses as many of them never wanted to test its authority over regulating cybersecurity. It was not until 2012 when a private company that had been victim to a cyber attack three times moved to dismiss the FTC's lawsuit, stating that it had no authority, rather than enter into a settlement. Going all the way up to the Third Circuit, the court affirmed that the FTC does in fact have the authority to regulate cybersecurity based on factors I won't bore you with here. Since then, there have been no direct challenges to the FTC's authority over a business's cybersecurity practices under this broad Section 5 and the FTC continues to use it repeatedly and effectively:

- Consent order with an education technology provider for alleged poor data security practices that exposed sensitive information about millions of customers and employees. Specifically, it did not require employees to use MFA, stored information insecurely, and failed to provide adequate security training to employees. – January, 2023

- Consent order with an online alcohol marketplace (and its CEO, personally) over allegations that its security failures led to a data breach exposing personal information of approximately 2.5M consumers. Specifically, it did not require employees to use MFA, did not limit employees' access to personal data, failed to monitor security threats, and stored information insecurely. – January, 2023
- Consent order with an online customized merchandise platform that failed to implement reasonable security measures and failed to adequately respond to several security breaches. Specifically, it stored SSN and passwords in readable text, did not require employees to use MFA , retained data longer than was reasonably necessary, and covered up major data breaches. – June, 2022

With the Safeguards Rule and the looming Motor Vehicle Trade Regulation Rule that the NADA is actively opposing, we believe that automotive retail is squarely in the sights of the new FTC commissioners. It is imperative that dealers continue in their efforts to expeditiously comply with all the new requirements of the Rule to achieve full compliance by the new deadline.

Contact: info@ComplyAuto.com
Website: www.complyauto.com

This article should be used as a compliance aid only and though its accuracy has been made a priority, it is not a substitute for professional legal advice. Each dealer should rely on their own expertise when using it.